BRIEFING PAPER

SUMS Consulting

working for universities, owned by universities

UNIVERSITY "GREY" USER IDENTITY MANAGEMENT

UNIVERSITY "GREY" USER IDENTITY MANAGEMENT

TABLE OF CONTENTS

1. INTRODUCTION 1

2. COMMON IDENTITY MANAGEMENT ISSUES 2

3. THE ROLE OF IT DEPARTMENTS IN IDENTITY MANAGEMENT 3

4. EXAMPLES OF GOOD PRACTICE 4

   POLICY: 4
   PROCESS: 4
   PEOPLE: 4
   SYSTEMS: 4

5. KEY PRINCIPLES FOR DEVELOPING IDENTITY MANAGEMENT 5

APPENDIX A – "GREY" USER CATEGORIES AND ELIGIBILITY 6

SUMS Consulting
Management Consultants

Suzie Moon
May 2014

1. Introduction

One of the main challenges currently facing university information management is to ensure that all the information held about an individual user is joined up across their different systems and that accurate digital identifiers are allocated to each of the individual university IT and library resource users. The requirements of electronic resource licence providers present further challenges as universities have to ensure that only the users permitted under the terms of their licence agreements are given access to the agreed, paid for, resources.

The resources and identifiers allocated to university staff and current students have been established by reference to university regulations, policies and practice. However, there remains a large number of users who are neither staff nor current students but who currently make a significant contribution to university life, teaching and research capability and who have a requirement to access ICT and library resources to a lesser or greater extent. These can include, for example, honorary staff, temporary staff, alumni, contractors, staff of university/business partnerships, and visitors – they are often referred to as “grey” users.

Lack of clarity around “grey” users can make it difficult for genuine contributors to access the required resources or easy for users with dubious authority to gain unauthorised access.

The following pages explore:

- Common Identity Management Issues
- The Role of IT departments in Identity Management
- Examples of Good Practice
- Key Principles for Developing Identity Management

If you have any questions about Identity Management please contact Suzie Moon or Bob Walder at SUMS Consulting:

Email: suzie.moon@reading.ac.uk or b.walder@reading.ac.uk

2. Common Identity Management Issues

SUMS' research has identified the following identify management issues:

- ***Ownership***: there needs to be clarity about where responsibility for "grey" user Identity Management lies within the university, particularly with regard to taking responsibility for an individual and the resources that the university provides for them – is it the IT or HR department, the library, the department or school or a combination of all or some of them?
- ***Compliance***: universities have to comply with current licensing, audit and data protection requirements. The increasing use of electronic resources, the majority of which are provided under strict licence terms, requires universities to demonstrate to the resource providers that users meet the stated criteria. Resource providers may withdraw access to resources for an institution if they find that licence terms have been breached and universities could also be open to potentially expensive legal action.
- ***Circumventing the system:*** sometimes an individual who has not received the access to ICT and/or library resources that they had requested or expected will try to circumvent the system by, for example, using someone else's university account information.
- ***Unclear university policies, processes and systems for Identity Management applicable to all users***: universities generally have developed clear policies and the processes and systems to successfully implement them with regard to their students and staff. However, this does not always extend to the "grey" users who now form a large part of a university community, especially with the growing trend for partner institutions within the UK and for building new campuses in other countries, particularly in the Far East.
- ***Sponsors do not follow current university policy***: sometimes the university sponsor for an individual seeking access to resources requests resource access which is not permitted under current university policy and this can cause friction and difficulty for the staff member who has to refuse or amend the request.
- ***Time consuming***: depending on the process being followed, particularly if it is paper based or part-paper based, requiring signatures from sponsors, it can take several days, even weeks for account access to be implemented which often leads to frustration and lack of productivity and does not present a picture of an efficient organisation to the end user who, in this digital age, expects to have their access needs arranged before they arrive at the university.
- ***Risk of paper based systems***: paper forms can and have been mislaid or delayed and sometimes, especially when granting a large number of permissions to a group perhaps at a training course or conference, they can be incorrectly completed which can lead to time-consuming chasing up or referring back to the originator.
- ***New funding arrangements:*** Since September 2012 universities have been funded by new arrangements which have seen a reduction in central grants and an increase in tuition fees, as well as new JISC banding categories which determine how much is paid for electronic resource licences and access. All sources of university income are now taken into account when determining bands and this includes funding from partners and overseas institutions. This may lead to increased expectations about access to university provided resources.
- ***Changes instituted by the resource providers***: Academic publishers and resource providers have introduced electronic systems which look at an individual's "defined values" as set by the institution in order to check that they match the criteria for the particular resource before access is provided, otherwise it will be denied. Universities need to ensure that individual user profiles are linked to the correct "values" which accord with current university policy and licence agreements or else provide facilities such as "walk-in" access to electronic resources which meet the licence provider's terms and conditions.

3. The Role of IT departments in Identity Management

University IT departments are responsible for setting up, maintaining and removing IT accounts, whether for students, staff or “grey” users. The policies and systems for provisioning student and staff accounts should be clearly set out in order to ensure the smooth functioning of registering students for the new academic year and the induction of a new member of university staff. This is not always the case however when university IT departments are asked to supply a “grey” user with an IT account and access to required resources.

The IT department will need to create or be provided with the following information before it is able to set up a new user account:

- A digital identity: unique to the individual user together with a unique user name and password
- A role: what does the individual do in the university e.g student, financial officer, IT Service Desk manager, etc.
- Entitlement(s): what university IT and academic resources the individual is able to access
- Authentication: demonstration that the individual requesting an identity and access to resources is who they say they are.

Often however a lack of clarity in these areas either causes delay or pushes access decisions onto staff who are not suitably qualified.

4. Examples of Good Practice

SUMS has recently conducted a number of comparator studies in order to determine good practice with regard to Identity Management, in universities, particularly with regard to “grey” users.

Policy:

- It is important that a clear policy is agreed and recognised regarding “grey” users and that their access permissions to resources and privileges is agreed and made explicit. This needs to be publicised to all staff members of the university.
- Honorary status is time limited
- Access to resources is based on the minimum needed to perform a role within the university.

Process:

- It is important to consider the requirements of any new Identity Management system including establishing the policies and processes before implementing new technology. This can be achieved by the creation of a special university group of stakeholders whose remit is to define user categories and consider entitlements and privileges as well as establishing a clear process to promote these as well as sanctions if they are not followed.
- “Associate” is the most common group name for “grey” users at a university
- Casual visitors’ details are currently not kept by university IT systems. Casual visitors have been given access to some universities’ public unsecure Wi-Fi systems which they can access by using their own email address.
- The library system can be used to check that a “grey” user has been given the correct authorisations that are permitted by the licence terms and can be used to give these authorisations direct to the “grey” user
- Departments become source owners and sponsor the “grey” user, and have to make the business case which justifies their use of university resources and systems and also take responsibility for their use of these resources
- An online Identity Management system can deal with an Associate request in a short time period (quickest could be a few minutes) if the required details and forms are completed promptly.

People:

- A series of university wide newsletters and workshops can been used to promote a new Identity Management system to relevant staff members and support its successful introduction. Staff who are involved are invited to give their feedback throughout the process.
- Creating a specific Identity Manager post can help in the management and creation of accounts and permissions.

Systems:

- A dedicated web site is essential to promote the Identity Management policies and procedures as well as giving guidance on Associate categories and resource and access rights
- An on-line based system that gives ownership to the sponsoring school or department can result in a much reduced time for creating an Associate account and allotting resources. It can also have other advantages as it means that information is held about the Associate which helps with other areas of university administration such as the giving out of parking permits. This may be useful when considering moves to a cloud based resource system with costs being able to be allocated back to the relevant sponsoring department.
- The new system of electronic resource providers relying on defined “values” means that some on-line resources are no longer available to some “grey” users. One solution is to provide one or more dedicated “walk-in” user” P.C.s in the university library.

5. Key Principles for Developing Identity Management

A number of key principles derived from good practice have been developed with regard to “grey” user Identity Management. These principles can be used as a basis to help inform the creation of a university “grey” user policy which should cover entitlements and groupings as well as the process for the creation and maintenance of “grey” user accounts:

- The allocation of resources and privileges to “grey” users at the university should be formally agreed as university policy
- A policy should contain a list of principles, a set of clearly defined categories and for each category a list of eligibilities. This could be extended to include all staff and students, both current and past, to create a university-wide Identity Management policy.
- The policy should contain a list of clearly defined roles, and for each role a single category into which it falls
- The policy should include how to deal with new “grey” user roles
- The policy needs to be well publicised to all university members and users as well as to future “grey” users and be publicly available on the university website
- All “grey” users, including honorary positions, should be time limited and resource and account privileges should be based on the individual’s role in the university
- The policy will need to be supported by clarifying processes and responsibilities
- Ownership of a “grey” user should be clearly established as part of university policy
- Provisions should be made to review, update and enforce the policy and institute disciplinary sanctions as required.

Completing a table based on the headings and exemplars suggested in Appendix A can form a useful resource to help clarify and develop “grey” user categories and eligibilities as well as indicating whether an individual is a “member” of the university as defined by its Charter.

Appendix A – “Grey” user categories and eligibility

“Grey” user categories and eligibility

Example “Grey” User	Needs access to which resources as a minimum	Able to access licensed /walk-in resources	University Sponsor	Review Period	University Member Y/N
Alumni	Alumni web pages. Internet when on University campus	Walk-in	Alumni Services	N/A	Y
Auditors	Internet; relevant systems access	Walk-in	Relevant Department	3 months	N
Casual Staff	Internet, then depends on role requirements	Walk-in	HR/Facilities	Annually	N
Contractors	Internet as minimum. May need access to email, software, data storage, relevant systems and library services	Licensed resources, only if their work requires access, otherwise walk-in	Relevant Department	3 months	N
Emeritus Appointments (Professors/Readers)	Internet, email, software and data storage, VLE and library services	Licensed resources	Relevant Department/Vice Chancellor’s	Annually	?
Office e.g. External Examiners	Internet. Access to examination papers and databases	Walk-in	Registry	3 Months	N